## CLAIMS

We claim:

1. A distributed access control system that restricts access to secured items, said system comprising:

a central server having a server module that provides overall access control; and

a plurality of local servers, each of said local servers including a local module that provides local access control,

wherein the access control, performed by said central server or said local servers, operates to permit or deny access requests to the secured items by requestors.

2. A distributed access control system as recited in claim 1, wherein said access control system couples to an enterprise network to restrict access to the secured files stored in a data storage device coupled to the enterprise network.

3. A distributed access control system as recited in claim 2, wherein the access requests are at least primarily processed in a distributed manner by said local servers.

4. A distributed access control system as recited in claim 3, wherein when the access requests are processed said local servers, the requestors gain access to the secured files without having to access said central server.

5. A distributed access control system as recited in claim 2, wherein the local module can be a copy of the server module so any of the local modules can operate independent of said central server and other of said local servers.

6. A distributed access control system as recited in claim 2, wherein the local module can be a subset of the server module.

7. A distributed access control system as recited in claim 2, wherein access permissions for said local servers can be dynamically configured to pass a requestor from one of said local servers to another of said local servers, thereby enabling access control to be performed by the another of said local servers such as when the location of the requestor changes.

8. A distributed access control system as recited in claim 2, wherein the secured items are secured files.

9. A distributed access control system as recited in claim 2, wherein the secured items are secured by encryption.

10. A method for providing access management through use of a plurality of server machines associated with different locations, said method comprising the acts of:

(a) authenticating a user with a first server machine of the plurality of server machines with respect to a prior access request;

(b) subsequently receiving a current access request to access a secured item via a second server machine of the plurality of server machines;

(c) reconfiguring the first server machine to prevent further access by the user to secured items via the first server machine; and

(d) reconfiguring the second server machine to permit access by the user to at least the secured item via the second server machine.

11. A method as recited in claim 10, wherein said authenticating (a) authenticates both the user and a client machine being used by the user.

12. A method as recited in claim 10, wherein the first server machine and the second server machine are access points for the user to gain access to secured items.

13. A method as recited in claim 10,

wherein when the user is at a first location, the user interacts over a network with the first server machine using a first client machine at the first location, and

wherein when the user is at a second location, the user interacts over a network with the second server machine using a second client machine at the second location.

14. A method as recited in claim 13, wherein said method further comprises at least the acts of:

(f) determining, prior to said reconfiguring (c) or (d), whether the user is permitted to gain access from a second location to secured items via the second server machine.

15. A method as recited in claim 13, wherein said authenticating (a) of the user occurs while the user is at a first location, and wherein said receiving (a) of the access request to access the secured item from the user occurs while the user is at a second location.

16. A method as recited in claim 16, wherein said method further comprises at least the acts of:

(e) determining permitted locations from which the user is permitted to gain access to secured documents;

(f) determining, prior to said reconfiguring (c) or (d), whether the second location is one of the permitted locations for the user; and

(g) bypassing said reconfiguring (c) or (d) when said determining (f) determines that the second location is not one of the permitted locations for the user.

17. A method as recited in claim 16,

wherein when the user is at the first location, the user interacts over a network with the first server machine using a first client machine at the first location, and

wherein when the user is at the second location, the user interacts over a network with the second server machine using a second client machine at the second location.

18. A computer readable medium including at least computer program code for providing access management through use of a plurality of server machines associated with different locations, said computer readable medium comprising:

computer program code for authenticating a user with a first server machine of the plurality of server machines with respect to a prior access request;

computer program code for subsequently receiving a current access request to access a secured item via a second server machine of the plurality of server machines;

computer program code for reconfiguring the first server machine to prevent further access by the user to secured items via the first server machine; and

computer program code for reconfiguring the second server machine to permit access by the user to at least the secured item via the second server machine.

19. A computer readable medium as recited in claim 18,

wherein when the user is at a first location, the user interacts over a network with the first server machine using a first client machine at the first location, and

wherein when the user is at a second location, the user interacts over a network with the second server machine using a second client machine at the second location.

20. A computer readable medium as recited in claim 19, wherein said method further comprises:

computer program code for determining, prior to the reconfiguring of either the first server machine or the second server machine, whether the user is permitted to gain access from a second location to secured items via the second server machine.